Arkansas Office of Information Technology
Mike Huckabee, Governor
Carolyn G. Walton, Executive CIO

Shared Technical Architecture
124 W. Capitol Ave. Suite 200
Little Rock, AR 72201

501.682.4300 Voice
501.682.2040 Fax
http://www.techarch.state.ar.us

Standard Statement – Personnel Security

Personnel Security	**Document Number:** SS-70-007
	Effective Date: xx/xx/2003
	Published By: Office of the ECIO

1.0 Purpose

All information assets handled by computer systems must be adequately protected against unauthorized modification, disclosure, or destruction. Personnel security is necessary to uphold access control and to limit information retrieval to a need to know basis.

2.0 Scope

This standard statement applies to all state agencies, institutions of higher education, boards and commissions.

3.0 Background

The Arkansas Information Systems Act of 1997 (Act 914, 1997) gives the Office of Information Technology the authority to define standards, policies and procedures to manage the information resources within the state. This is accomplished through work with a multi-agency working group known as the Shared Technical Architecture Team.

In addition, Act 1042 of 2001 states that the Executive Chief Information Officer oversees the development of information technology security policy for state agencies.

4.0 References

4.1 Act 914 of 1997: Authorized the Office of Information Technology (OIT) to develop statewide policies.

4.2 Act 1042 of 2001: Authorized the Executive CIO to develop security policy.

5.0 Standard

5.1 Each affected organization shall implement an ongoing IT security awareness program which communicates the IT security policy to each user and promotes a complete understanding of the importance of IT security. It should convey the message that IT security is to the benefit of the organization and all its employees, and that all employees are responsible for IT security.

5.2 IT management should ensure that their personnel, including contracted personnel, are subjected to an appropriate level of security clearance before they are hired, transferred or promoted, depending on the sensitivity of the position. A employee who was not subjected to such a clearance when first hired, should not be placed in a sensitive position until a security clearance has been obtained.

5.3 IT management should maintain a record of individuals currently authorized to access sensitive information.

5.4 IT management should ensure that operations and maintenance personnel, such as vendors or other service providers, have appropriate access to IT resources.

6.0 Procedures

The agency shall be able to demonstrate compliance with this policy.

7.0 Revision History

Date	Description of Change

8.0 Definitions

8.1 Training: Any information sharing, orientation process, ongoing supervision, or counseling. This may also include training by methods of an informal classroom, the intranet, and any posted internet information.

8.2 Security Clearance: Security clearance may include a law enforcement background check and may be combined with some form of biometric identification (i.e., fingerprints)

9.0 Resources

9.1 COBIT Standards: http://www.isaca.org/cobit.htm
9.2 HIPAA Security Standards: http://www.hipaadvisory.com/regs/finalsecurity/
9.3 United States Department of Agriculture's Personnel Security Process: http://www.usda.gov/da/ocpm/Web-PESE.htm#Types

10.0 Inquiries

Direct inquiries about this policy to:

Office of Information Technology
Shared Technical Architecture
124 W. Capitol Ave., Suite 200
Little Rock, AR 72201
Voice: 501-682-4300
FAX: 501-682-2040
Email: ITarch@mail.state.ar.us
OIT policies can be found on the Internet at:
http://www.techarch.state.ar.us